

ON THE FLAT COHOMOLOGY OF BINARY NORM FORMS

RONY A. BITAN AND MICHAEL M. SCHEIN

ABSTRACT. Given a quadratic number field $k = \mathbb{Q}(\sqrt{d})$ with narrow class number h_d^+ and discriminant Δ_k , let $\underline{\mathbf{O}}_d$ be the orthogonal \mathbb{Z} -group of the associated norm form q_d . In this paper we describe the structure of the pointed set $H_{\text{fl}}^1(\mathbb{Z}, \underline{\mathbf{O}}_d)$, which classifies quadratic forms isomorphic (properly or improperly) to q_d in the flat topology, and express its cardinality in terms of h_d^+ and h_d^- . Using this cohomological language we extend the classical result of Gauss that the composition of any form of discriminant Δ_k with itself belongs to the principal genus.

1. INTRODUCTION

Let $k = \mathbb{Q}(\sqrt{d})$ be a quadratic field with discriminant Δ_k ; here $d \notin \{0, 1\}$ is a square-free integer. Gauss showed in his famous *Disquisitiones Arithmeticae* [Gau] that the narrow class group $\text{Pic}^+(\mathcal{O}_k)$ of k , properly (i.e., with $\det = 1$ isomorphisms) classifies binary integral quadratic forms of discriminant Δ_k . A modern perspective on this classical idea, used in the 1980's by Ono [Ono2] for number fields and extended by Morishita [Mor] to general global fields, observes that the integral model of the norm torus associated to k/\mathbb{Q} , induced by the ring extension \mathcal{O}_k/\mathbb{Z} , is the special orthogonal group of the associated integral norm form q_d , and that its first flat cohomology set over \mathbb{Z} classifies binary integral quadratic forms of discriminant Δ_k . Analogously, the first Nisnevich cohomology set classifies forms in the principal genus. In this paper we extend this approach to arbitrary quadratic orders $\mathcal{O} \subseteq \mathcal{O}_k$ and then use flat cohomology, including a recent result of Gille [Gil], to obtain a total classification (not up to proper isomorphism), in terms of the Picard group $\text{Pic } \mathcal{O}$, of integral forms that are locally isomorphic for the flat topology to the norm form associated to certain orders \mathcal{O}/\mathbb{Z} .

If $\underline{\mathbf{O}}_d$ is the orthogonal group of q_d , the proper classification, which is represented due to Gauss by $\text{Pic}^+(\mathcal{O}_k)$, need not inject into the total one given by $H_{\text{fl}}^1(\mathbb{Z}, \underline{\mathbf{O}}_d)$. On the other hand, we shall see in (4.1) that if $d \equiv 2, 3 \pmod{4}$, then $H_{\text{fl}}^1(\mathbb{Z}, \underline{\mathbf{O}}_d)$ contains classes of forms of discriminant $-\Delta_k$. This phenomenon does not occur if $d \equiv 1 \pmod{4}$, in which case q_d is non-diagonal.

After establishing some facts concerning the special orthogonal group \underline{N}_d of q_d in the next two sections, we obtain in Section 4 a description of the finite groups $\underline{\mathbf{O}}_d/\underline{N}_d$, which turns out to depend

This work was supported by grant 1246/2014 from the Germany-Israel Foundation. The first author was also supported by a Chateaubriand Fellowship of the Embassy of France in Israel, 2016.

only on the residue of d modulo 4. From this we deduce the structure of $H_{\text{fl}}^1(\mathbb{Z}, \underline{\mathcal{O}}_d)$ in the final section. We show (Lemma 5.5 and Corollary 5.11) that:

$$H_{\text{fl}}^1(\mathbb{Z}, \underline{\mathcal{O}}_d) = \begin{cases} H_{\text{fl}}^1(\mathbb{Z}, \underline{N}_d) & d \equiv 1 \pmod{4} \\ (H_{\text{fl}}^1(\mathbb{Z}, \underline{N}_d) / \sim) \amalg (H_{\text{fl}}^1(\mathbb{Z}, \underline{N}'_{-d}) / \sim) & d \equiv 2, 3 \pmod{4}. \end{cases} \quad (1.1)$$

Here the abelian groups $H_{\text{fl}}^1(\mathbb{Z}, \underline{N}_d)$ and $H_{\text{fl}}^1(\mathbb{Z}, \underline{N}'_{-d})$ properly classify integral forms that are locally isomorphic for the flat topology to the forms $x^2 - dy^2$ and $x^2 + dy^2$, respectively; the equivalence relation \sim is determined by $[ax^2 + bxy + cy^2] \sim [ax^2 - bxy + cy^2]$. Moreover, we show in Lemma 5.12 that, for any d ,

$$H_{\text{fl}}^1(\mathbb{Z}, \underline{N}_d) = \{\pm 1\}^{\mu(d)} \times \text{Pic}^+(\mathcal{O}_k), \text{ where } \mu(d) := \begin{cases} 1 & d < 0 \\ 0 & d > 0. \end{cases}$$

The same is true for $\mathbb{Z}[\sqrt{d}]$ when $d \equiv 1 \pmod{4}$, cf. Proposition 5.13. This description leads to a formula expressing the cardinality of $H_{\text{fl}}^1(\mathbb{Z}, \underline{\mathcal{O}}_d)$ in terms of h_d^+ and h_{-d}^+ (Proposition 5.14). Furthermore, we show in Corollary 5.15 that any \underline{N}_d -torsor, tensored with itself, belongs to the principal genus of q_d . This may be viewed as an extension, in the language of cohomology, of another well-known theorem of Gauss about $\text{Pic}^+(\mathcal{O}_k)$.

Acknowledgements: The authors thank B. Conrad, P. Gille and B. Kunyavskiĭ for valuable discussions concerning the topics of the present article.

2. PRELIMINARIES

Let k/\mathbb{Q} be a Galois extension with Galois group $\Gamma = \text{Gal}(k/\mathbb{Q})$ and degree $n = [k : \mathbb{Q}]$. Let \mathbb{G}_m and \mathbf{GL}_n denote the multiplicative and general linear \mathbb{Z} -groups, respectively. Fixing a \mathbb{Z} -basis $\Omega = \{\omega_1, \dots, \omega_n\}$ for an *order* (i.e. a \mathbb{Z} -lattice of maximal rank) $\mathcal{O}_\Omega \subseteq \mathcal{O}_k$, we obtain an embedding $\iota : \underline{R}_\Omega := \text{Res}_{\mathcal{O}_\Omega/\mathbb{Z}}(\mathbb{G}_m) \hookrightarrow \mathbf{GL}_n$, where $\text{Res}_{\mathcal{O}_\Omega/\mathbb{Z}}(\mathbb{G}_m)$ denotes the Weil restriction of scalars (see [BLR, §7.6]). Composition with the determinant provides a map $\underline{R}_\Omega \rightarrow \mathbb{G}_m$, which we abusively denote \det . Let $\rho : \mathcal{O}_\Omega^\times \simeq \underline{R}_\Omega(\mathbb{Z})$ be the natural isomorphism, so that $N_{k/\mathbb{Q}}(\alpha) = \det(\iota(\rho(\alpha)))$ for all $\alpha \in \mathcal{O}_\Omega^\times$; see Exercise 9(c) of [Bou, Section II.5]. We obtain a short exact sequence of \mathbb{Z} -groups:

$$1 \rightarrow \underline{N}_\Omega \rightarrow \underline{R}_\Omega \xrightarrow{\det} \mathbb{G}_m \rightarrow 1, \quad (2.1)$$

whose generic fibers are the norm torus $N := \text{Res}_{k/\mathbb{Q}}^{(1)}(\mathbb{G}_m)$, the Weil torus $R := \text{Res}_{k/\mathbb{Q}}(\mathbb{G}_m)$, and the multiplicative \mathbb{Q} -group \mathbb{G}_m , respectively. Their geometric fibers at any prime p are denoted by $(\underline{N}_\Omega)_p$, $(\underline{R}_\Omega)_p$ and $(\mathbb{G}_m)_p$, respectively, whilst their reductions are overlined. If \mathcal{O}_Ω is the maximal order \mathcal{O}_k , we omit the subscript Ω . The groups of \mathbb{Z} -points of these integral models are the maximal compact subgroups of $N(\mathbb{Q})$, $R(\mathbb{Q})$ and \mathbb{Q}^\times , respectively.

While $\underline{\mathbb{G}}_m$ and \underline{R}_Ω are smooth over $\text{Spec } \mathbb{Z}$, the kernel \underline{N}_Ω need not be smooth, in the sense that it may have a non-reduced reduction at some prime. So instead of using étale cohomology, we shall restrict ourselves to flat cohomology. To this end we shall need the following lemma.

Lemma 2.1. *The scheme \underline{N}_Ω is flat over $\text{Spec } \mathbb{Z}$.*

Proof. We wish to apply the Miracle Flatness Theorem [Mat, Theorem 23.1] to the map $\det : \underline{R}_\Omega \rightarrow \underline{\mathbb{G}}_m$ from the sequence (2.1). As the two schemes are smooth, hence regular and Cohen-Macaulay, it suffices to check that all geometric fibers of $\underline{N}_\Omega = \ker(\det)$ have the same dimension $[k : \mathbb{Q}] - 1$. The only thing to verify is that the map $\det : (\overline{R}_\Omega)_p \xrightarrow{\det_p} (\overline{\mathbb{G}}_m)_p$ in the reduction of sequence (2.1) is not trivial for any p . But this is clear since \det is surjective. \square

Applying flat cohomology to (2.1) gives rise to a long exact sequence of pointed sets (see [Gir, Proposition 3.3.1.(i)]):

$$1 \rightarrow \underline{N}_\Omega(\mathbb{Z}) \rightarrow \underline{R}_\Omega(\mathbb{Z}) \cong \mathcal{O}_\Omega^\times \xrightarrow{N_{k/\mathbb{Q}}} \{\pm 1\} \rightarrow H_{\text{fl}}^1(\mathbb{Z}, \underline{N}_\Omega) \rightarrow H_{\text{fl}}^1(\mathbb{Z}, \underline{R}_\Omega) \rightarrow H_{\text{fl}}^1(\mathbb{Z}, \underline{\mathbb{G}}_m) = \text{Pic } (\mathbb{Z}) = 0. \quad (2.2)$$

By Shapiro's Lemma [SGA3, XXIV, Prop. 8.2] we have $H_{\text{fl}}^1(\mathbb{Z}, \underline{R}_\Omega) \cong H_{\text{fl}}^1(\mathcal{O}_\Omega, \underline{\mathbb{G}}_{m, \mathcal{O}_\Omega}) = \text{Pic } (\mathcal{O}_\Omega)$. Thus (2.2) can be rewritten as

$$1 \rightarrow \{\pm 1\}/N_{k/\mathbb{Q}}(\mathcal{O}_\Omega^\times) \rightarrow H_{\text{fl}}^1(\mathbb{Z}, \underline{N}_\Omega) \rightarrow \text{Pic } (\mathcal{O}_\Omega) \rightarrow 1. \quad (2.3)$$

The maximal order \mathcal{O}_k is a Dedekind domain, whence its Picard group coincides with the ideal class group of k . The set $\{\pm 1\}/N_{k/\mathbb{Q}}(\mathcal{O}_k^\times)$ is equal to the zero-Tate cohomology set $H_T^0(\Gamma, \mathcal{O}_k^\times)$ (see [Ono2, Example 1]). Thus, in the case $\mathcal{O}_\Omega = \mathcal{O}_k$, we deduce an isomorphism of finite groups

$$H_{\text{fl}}^1(\mathbb{Z}, \underline{N})/H_T^0(\Gamma, \mathcal{O}_k^\times) \cong \text{Pic } (\mathcal{O}_k). \quad (2.4)$$

If n is odd, then $N_{k/\mathbb{Q}}(-1) = (-1)^n = -1$. Therefore: $H_{\text{fl}}^1(\mathbb{Z}, \underline{N}) \cong \text{Pic } (\mathcal{O}_k)$ and it follows that

$$h_k = |H_{\text{fl}}^1(\mathbb{Z}, \underline{N})|. \quad (2.5)$$

In the quadratic case $n = 2$, we have $k = \mathbb{Q}(\sqrt{d})$ for some square-free integer $d \notin \{0, 1\}$. If \mathcal{O}_Ω is the maximal order \mathcal{O}_k , we set h_d and \underline{N}_d to be the class number h_k and the \mathbb{Z} -group \underline{N} , respectively. Then (2.3) implies

$$|H_{\text{fl}}^1(\mathbb{Z}, \underline{N}_d)| = h_d \cdot 2^{\varepsilon(d)}, \quad (2.6)$$

where [Ono2, §5, Example 2]:

$$\varepsilon(d) := \begin{cases} 1 & d < 0 \text{ or } (d > 0 \text{ and } N_{k/\mathbb{Q}}(\mathcal{O}_k^\times) = \{1\}) \\ 0 & \text{otherwise.} \end{cases} \quad (2.7)$$

Let $\text{Pic}^+(\mathcal{O}_k)$ be the narrow class group of k and let h_d^+ denote its cardinality. It is equal to h_d unless $d > 0$ and $N_{k/\mathbb{Q}}(\mathcal{O}_k^\times) = \{1\}$, in which case $h_d^+ = 2h_d$, and so (2.6) simplifies to

$$|H_{\mathfrak{H}}^1(\mathbb{Z}, \underline{N}_d)| = h_d^+ \cdot 2^{\mu(d)}, \quad \mu(d) := \begin{cases} 1 & d < 0 \\ 0 & d > 0. \end{cases} \quad (2.8)$$

Hence computing the narrow class number h_d^+ is equivalent to determining $|H_{\mathfrak{H}}^1(\mathbb{Z}, \underline{N}_d)|$.

3. THE CLASS SET OF THE NORM TORUS

Let \underline{G} be an affine flat group scheme defined over $\text{Spec } \mathbb{Z}$ with generic fiber G . The geometric fiber of \underline{G} at the prime p , namely its extension to $\text{Spec } \mathbb{Z}_p$, is denoted by \underline{G}_p . We consider the adelic group $\underline{G}(\mathbb{A})$ and its subgroup $\underline{G}(\mathbb{A}_\infty)$ over the *ring of integral adèles* $\mathbb{A}_\infty := \mathbb{R} \times \prod_p \mathbb{Z}_p$.

Definition 1. The *class set* of \underline{G} is the set of double cosets $\text{Cl}_\infty(\underline{G}) := \underline{G}(\mathbb{A}_\infty) \backslash \underline{G}(\mathbb{A}) / G(\mathbb{Q})$. This set is finite ([BP, Prop. 3.9]) and its cardinality, denoted by $h(\underline{G})$, is called the *class number* of \underline{G} .

Definition 2. Let S be a finite set of places in \mathbb{Q} . The *first Tate-Shafarevich group* of G over \mathbb{Q} relative to S is:

$$\text{III}_S^1(\mathbb{Q}, G) := \ker \left[H^1(\mathbb{Q}, G) \rightarrow \prod_{v \notin S} H^1(\mathbb{Q}_v, G_v) \right].$$

When $S = \emptyset$, we simply write $\text{III}^1(\mathbb{Q}, G)$.

Remark 3.1. Let \underline{G} be an affine, flat, and finitely generated \mathbb{Z} -group scheme. Y. Nisnevich [Nis, Theorem I.3.5.] proved that there exists an exact sequence of pointed sets

$$1 \rightarrow \text{Cl}_\infty(\underline{G}) \rightarrow H_{\mathfrak{H}}^1(\mathbb{Z}, \underline{G}) \rightarrow H^1(\mathbb{Q}, G) \times \prod_p H_{\mathfrak{H}}^1(\mathbb{Z}_p, \underline{G}_p) \quad (3.1)$$

whose left exactness reflects the fact that $\text{Cl}_\infty(\underline{G})$ is the set of twisted \mathbb{Z} -forms of \underline{G} that are isomorphic to \underline{G} over some flat extension of \mathbb{Z} and over some flat extension of \mathbb{Z}_p for all p . If $H_{\mathfrak{H}}^1(\mathbb{Z}_p, \underline{G}_p)$ injects into $H^1(\mathbb{Q}_p, G_p)$ for any p , this sequence simplifies to

$$1 \rightarrow \text{Cl}_\infty(\underline{G}) \rightarrow H_{\mathfrak{H}}^1(\mathbb{Z}, \underline{G}) \rightarrow H^1(\mathbb{Q}, G). \quad (3.2)$$

More precisely, there is an exact sequence of pointed sets (cf. [GP, Corollary A.8])

$$1 \rightarrow \text{Cl}_\infty(\underline{G}) \rightarrow H_{\mathfrak{H}}^1(\mathbb{Z}, \underline{G}) \rightarrow B \rightarrow 1 \quad (3.3)$$

in which

$$B = \{[\gamma] \in H^1(\mathbb{Q}, G) : [\gamma \otimes \mathbb{Z}_p] \in \text{Im}(H_{\mathfrak{H}}^1(\mathbb{Z}_p, \underline{G}_p) \rightarrow H^1(\mathbb{Q}_p, G_p)) \quad \forall p\}.$$

Let p be a rational prime, and let P be a prime of k dividing p . Since k/\mathbb{Q} is a Galois extension, the local field k_P is independent of the choice of P , up to isomorphism. Observe that $k \otimes_{\mathbb{Q}} \mathbb{Q}_p \cong k_P^r$, where r is the number of primes of k dividing p . The norm map $N_{k/\mathbb{Q}}$ induces a map $\text{Nr} : k \otimes_{\mathbb{Q}} \mathbb{Q}_p \rightarrow \mathbb{Q}_p$; under the isomorphism above this corresponds to the product of the norm maps N_{k_P/\mathbb{Q}_p} on the components. Similarly, $\mathcal{O}_k \otimes_{\mathbb{Z}} \mathbb{Z}_p \simeq \mathcal{O}_{k_P}^r$. Write U_P for $\mathcal{O}_{k_P}^\times$.

Applying flat cohomology to the short exact sequence of flat \mathbb{Z}_p -groups

$$1 \rightarrow \underline{N}_p \rightarrow \underline{R}_p \rightarrow (\mathbb{G}_m)_p \rightarrow 1$$

yields the exact sequence

$$1 \rightarrow \underline{N}_p(\mathbb{Z}_p) \rightarrow \underline{R}_p(\mathbb{Z}_p) \cong U_P^r \xrightarrow{\text{Nr}} \mathbb{Z}_p^\times \rightarrow H_{\text{fl}}^1(\mathbb{Z}_p, \underline{N}_p) \rightarrow 1,$$

since $H_{\text{fl}}^1(\mathbb{Z}_p, \underline{R}_p)$ is the Picard group of a product of local rings and thus vanishes. We deduce that $H_{\text{fl}}^1(\mathbb{Z}_p, \underline{N}_p) \cong \mathbb{Z}_p^\times / \text{Nr}(U_P^r) = \mathbb{Z}_p^\times / N_{k_P/\mathbb{Q}_p}(U_P)$. Applying Galois cohomology to the short exact sequence of \mathbb{Q}_p -groups

$$1 \rightarrow N_p \rightarrow R_p \rightarrow (\mathbb{G}_m)_p \rightarrow 1$$

gives rise to the exact sequence of abelian groups

$$1 \rightarrow N_p(\mathbb{Q}_p) \rightarrow R_p(\mathbb{Q}_p) \cong (k_P^\times)^r \xrightarrow{\text{Nr}} \mathbb{Q}_p^\times \rightarrow H^1(\mathbb{Q}_p, N_p) \rightarrow 1,$$

where the rightmost term vanishes by Hilbert's Theorem 90. Hence $H^1(\mathbb{Q}_p, N_p) \cong \mathbb{Q}_p^\times / N_{k_P/\mathbb{Q}_p}(k_P^\times)$. Note that U_P is compact and thus $N_{k_P/\mathbb{Q}_p}(U_P)$ is closed in \mathbb{Q}_p^\times . Only units have norms that are units, so we obtain an embedding of groups:

$$H_{\text{fl}}^1(\mathbb{Z}_p, \underline{N}_p) \cong \mathbb{Z}_p^\times / N_{k_P/\mathbb{Q}_p}(U_P) \hookrightarrow \mathbb{Q}_p^\times / N_{k_P/\mathbb{Q}_p}(k_P^\times) \cong H^1(\mathbb{Q}_p, N_p). \quad (3.4)$$

Corollary 3.2. *Suppose k/\mathbb{Q} is cyclic. Let S_r be the set of primes dividing Δ_k . Then there is an exact sequence of abelian groups (compare with Formula (5.3) in [Mor]):*

$$1 \rightarrow \text{Cl}_\infty(\underline{N}) \rightarrow H_{\text{fl}}^1(\mathbb{Z}, \underline{N}) \rightarrow \text{III}_{S_r \cup \{\infty\}}^1(\mathbb{Q}, N) \rightarrow 1.$$

Proof. Since $H_{\text{fl}}^1(\mathbb{Z}_p, \underline{N}_p)$ embeds into $H^1(\mathbb{Q}_p, N_p)$ for any prime p by (3.4), the \mathbb{Z} -group scheme \underline{N} admits the exact sequence (3.3), in which the terms are abelian groups as \underline{N} is commutative. The pointed set $\text{Cl}_\infty(\underline{N})$ is bijective to the first Nisnevich cohomology set $H_{\text{Nis}}^1(\mathbb{Z}, \underline{N})$ (cf. [Nis, I. Theorem 2.8]), which is a subgroup of $H_{\text{fl}}^1(\mathbb{Z}, \underline{N})$ because any Nisnevich cover is flat. Hence the first map is an embedding. As k/\mathbb{Q} is abelian, at any prime p the local Artin reciprocity law (cf. [Mil, I. Theorem 1.1]) implies that:

$$n_p = |\text{Gal}(k_p/\mathbb{Q}_p)| = [\mathbb{Q}_p^\times : N_{k_p/\mathbb{Q}_p}(k_P^\times)] = |H^1(\mathbb{Q}_p, N_p)|.$$

Furthermore, this rule shows that $|H_{\text{fl}}^1(\mathbb{Z}_p, \underline{N}_p)| = [U_p : N_{k_p/\mathbb{Q}_p}(U_p)]$ equals the ramification index e_p (see [KCon, Theorem 7.6]). So if k/\mathbb{Q} is cyclic, for which at any p ramification is totally ramification, e_p is n_p at ramified places and 1 elsewhere. This means following (3.4) that $H_{\text{fl}}^1(\mathbb{Z}_p, \underline{N}_p)$ coincides with $H^1(\mathbb{Q}_p, N_p)$ at ramified primes p and vanishes elsewhere. Thus B consists of classes $[\gamma] \in H^1(\mathbb{Q}, N)$ whose geometric fibers vanish at unramified places, i.e., $B = \text{III}_{S_r \cup \{\infty\}}^1(\mathbb{Q}, N)$. \square

Remark 3.3. The group $B = \text{III}_{S_r \cup \{\infty\}}^1(\mathbb{Q}, N)$ can be embedded in $\prod_{v \in S_r \cup \{\infty\}} H^1(\mathbb{Q}_v, N_v)$, as can be seen by applying the Snake Lemma to the following exact diagram (cf. [Mor, p.140]):

$$\begin{array}{ccccc} H^1(\mathbb{Q}, N) & \xlongequal{\quad} & H^1(\mathbb{Q}, N) & & \\ \downarrow l & & \downarrow m & & \\ \prod_{v \in S_r \cup \{\infty\}} H^1(\mathbb{Q}_v, N_v) & \hookrightarrow & \prod_v H^1(\mathbb{Q}_v, N_v) & \twoheadrightarrow & \prod_{v \notin S_r \cup \{\infty\}} H^1(\mathbb{Q}_v, N_v) \end{array}$$

in which $\ker(l) = \text{III}^1(\mathbb{Q}, N) = 0$ for cyclic k/\mathbb{Q} by the Hasse Norm Theorem [Ono1, Prop. 4.5.1], and $B = \ker(m)$. In particular, if $[k : \mathbb{Q}] = n$ is prime, then B has exponent n .

4. NORM FORMS OF QUADRATIC NUMBER FIELDS

Throughout the rest of this paper we will assume that k is a quadratic number field, so that $k = \mathbb{Q}(\sqrt{d})$, where $d \notin \{0, 1\}$ is a square-free integer. Recall that a *binary integral quadratic form* is a homogeneous polynomial of order two in two variables. with coefficients in \mathbb{Z} :

$$q : \mathbb{Z}^2 \rightarrow \mathbb{Z}; \quad q(x, y) = ax^2 + bxy + cy^2, \quad a, b, c \in \mathbb{Z}.$$

The form q is represented by the symmetric 2×2 matrix $B_q = \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}$ satisfying $q(x, y) = (x, y)^t B_q (x, y)$. We denote q by the triple (a, b, c) . The *discriminant* of q is the *integer* $b^2 - 4ac$. Two integral forms q and q' are said to be \mathbb{Z} -*isomorphic* if there exists $A \in \underline{\mathbf{GL}}_2(\mathbb{Z})$ such that $q \circ A = q'$; this means that $q(A(x, y)) = q'(x, y)$ for all $x, y \in \mathbb{Z}$. This condition can be stated equivalently as $A^t B_q A = B_{q'}$. Such a matrix A is called an *isometry*. If $\det A = 1$, then we say that A gives a *proper isomorphism* between q and q' .

Definition 3. The *orthogonal group scheme* of q is the \mathbb{Z} -group of its self-isometries:

$$\underline{\mathbf{O}}_q := \{A \in \underline{\mathbf{GL}}_2 : q \circ A = q\}.$$

Note that $\det A = \pm 1$ for all $A \in \underline{\mathbf{O}}_q$.

Definition 4. Let $\Omega = \{\omega_1, \omega_2\} \subset \mathcal{O}_k$ be a basis of a quadratic order $\mathcal{O}_\Omega \subseteq \mathcal{O}_k$. The *norm form* associated to Ω is the integral quadratic form:

$$q_\Omega(x, y) := N_{k/\mathbb{Q}}(x\omega_1 + y\omega_2), \quad \forall x, y \in \mathbb{Z}.$$

Let $\underline{\mathbf{O}}_\Omega$ be the orthogonal group of q_Ω , and let $\underline{\mathbf{O}}_\Omega^+$ be the subgroup consisting of matrixes with determinant 1.

Lemma 4.1. *Let Ω be a basis of the quadratic order $\mathcal{O}_\Omega \subseteq \mathcal{O}_k$. Then $\underline{\mathbf{O}}_\Omega^+ = \underline{N}_\Omega$.*

Proof. Observing the commutative diagrams

$$\begin{array}{ccc} \mathbb{Z}^2 & \xrightarrow[r \cong]{r} & \mathcal{O}_\Omega \\ \downarrow q_\Omega & & \downarrow N_{k/\mathbb{Q}} \\ \mathbb{Z} & \xlongequal{\quad} & \mathbb{Z} \end{array} \quad \begin{array}{ccc} \underline{\text{Aut}}(\mathcal{O}_\Omega) & \xrightarrow[\cong]{\rho} & \underline{R}_\Omega \\ \downarrow N_{k/\mathbb{Q}} & & \downarrow \det \\ \underline{\mathbb{G}}_m & \xlongequal{\quad} & \underline{\mathbb{G}}_m \end{array}$$

in which $r(x, y) = \omega_1 x + \omega_2 y$, we see that

$$\begin{aligned} \underline{\mathbf{O}}_\Omega^+ &= \{A \in \underline{\mathbf{GL}}_2 : q_\Omega \circ A = q_\Omega, \det(A) = 1\} \\ &= \{a \in \underline{\text{Aut}}(\mathcal{O}_\Omega) : N_{k/\mathbb{Q}} \circ a = N_{k/\mathbb{Q}}, N_{k/\mathbb{Q}}(a) = 1\} \\ &= \{B \in \underline{R}_\Omega : \det(B) = 1\} = \underline{N}_\Omega. \end{aligned} \quad \square$$

Let q_d be the norm form associated to the basis $\Omega = \{1, \omega\}$ of the maximal order \mathcal{O}_k . It is well-known that we may take $\omega = \frac{1+\sqrt{d}}{2}$ if $d \equiv 1 \pmod{4}$ and $\omega = \sqrt{d}$ otherwise. Then

$$q_d = \begin{cases} (1, 1, c) & d \equiv 1 \pmod{4} \\ (1, 0, -d) & d \equiv 2, 3 \pmod{4} \end{cases} \quad \text{and} \quad B_{q_d} = \begin{cases} \begin{pmatrix} 1 & 1/2 \\ 1/2 & c \end{pmatrix} & d \equiv 1 \pmod{4} \\ \begin{pmatrix} 1 & 0 \\ 0 & -d \end{pmatrix} & d \equiv 2, 3 \pmod{4}, \end{cases} \quad (4.1)$$

where $c = \frac{1-d}{4}$. Hence

$$\underline{N}_d = \begin{cases} \text{Spec } \mathbb{Z}[x, y] / (x^2 + xy + cy^2 - 1) & d \equiv 1 \pmod{4}, \\ \text{Spec } \mathbb{Z}[x, y] / (x^2 - dy^2 - 1) & d \equiv 2, 3 \pmod{4}. \end{cases}$$

The integral matrix realization $\iota(\underline{N}_d(\mathbb{Z}))$ is given by

$$A_d = \begin{cases} \begin{pmatrix} x & -cy \\ y & x+y \end{pmatrix} : \det = 1 & d \equiv 1 \pmod{4}, \\ \begin{pmatrix} x & dy \\ y & x \end{pmatrix} : \det = 1 & d \equiv 2, 3 \pmod{4}. \end{cases} \quad (4.2)$$

These two integral models of N , being flat (see Remark 2.1), share the same generic fiber

$$N = \underline{N}_d \otimes_{\text{Spec } \mathbb{Z}} \mathbb{Q} = \text{Spec } \mathbb{Q}[x, y] / (x^2 - dy^2 - 1).$$

5. THE FLAT COHOMOLOGY OF THE ORTHOGONAL GROUP OF A NORM FORM

Let $\underline{\mathbf{O}}_d$ be the orthogonal group of the norm form q_d with generic fiber $\mathbf{O}_d = \underline{\mathbf{O}}_d \otimes_{\mathrm{Spec} \mathbb{Z}} k$. Since \underline{N}_d is the intersection of $\underline{\mathbf{O}}_d$ with $\underline{\mathbf{SL}}_2$, one might have expected \underline{N}_d to be the kernel of $\underline{\mathbf{O}}_d \xrightarrow{\det} \underline{\mu}_2$. However, this need not be true: the map \det may not be flat locally at (2), thus not producing a flat kernel (see B. Conrad's notes [BCon, Cor. 2.7]), whereas \underline{N}_d is flat by Lemma 2.1. So we ask whether $\underline{\mathbf{O}}_d/\underline{N}_d$ is affine and whether it is a finite group scheme.

Lemma 5.1. *A separated flat group scheme \underline{G} of finite type over a Dedekind ring is finite if and only if all fibers are affine and finite of a constant rank.*

Proof. The direct direction is obvious. Conversely, if all fibers are affine, then [SGA3, VIB, Proposition 12.10.(iii)] yields that the map $\underline{G} \rightarrow \underline{G}_{\mathrm{af}}$ is an isomorphism. Hence \underline{G} is affine. \square

Both $\underline{\mathbf{O}}_d$ and \underline{N}_d are affine and flat of the same dimension, since $\underline{\mathbf{O}}_d$ is a union of \underline{N}_d and $a_d \underline{N}_d$, where $a_d \in \underline{\mathbf{O}}_d$ is an element of order two. For instance, we may take

$$a_d = \begin{cases} \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix} & d \equiv 1 \pmod{4}, \\ \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} & d \equiv 2, 3 \pmod{4}. \end{cases} \quad (5.1)$$

Thus $\underline{\mathbf{O}}_d/\underline{N}_d$ is separated and of finite type and its rank remains 2 locally everywhere. So it is finite by Lemma 5.1. Up to isomorphism, there are only two finite \mathbb{Z} -groups of order 2, namely $(\mathbb{Z}/2)_{\mathbb{Z}} := \mathrm{Spec} \mathbb{Z}[t]/(t^2 - t)$ and $\underline{\mu}_2 := \mathrm{Spec} \mathbb{Z}[t]/(t^2 - 1)$; see, for instance, [TO, p.21, Corollary]. These two \mathbb{Z} -groups are locally isomorphic everywhere except for at (2), in which case $\underline{\mu}_2 \otimes_{\mathrm{Spec} \mathbb{Z}} \mathbb{F}_2$ contains one nilpotent point while $(\mathbb{Z}/2)_{\mathbb{Z}} \otimes_{\mathrm{Spec} \mathbb{Z}} \mathbb{F}_2$ is reduced and contains two points.

Remark 5.2. The short exact sequence of \mathbb{Z} -groups

$$1 \rightarrow \underline{N}_d \rightarrow \underline{\mathbf{O}}_d \rightarrow \underline{\mathbf{O}}_d/\underline{N}_d \rightarrow 1$$

splits. Indeed, one may consider the section mapping the non-trivial element in $\underline{\mathbf{O}}_d/\underline{N}_d$ to a_d .

We now establish a basic result that will be used later.

Lemma 5.3. *Let d be any integer. The ring $\mathbb{Z}[\sqrt{d}]$ has a unique prime ideal containing 2.*

Proof. The case $d \in \{0, 1\}$ is obvious, so we assume that it does not hold. We may assume without loss of generality that d is square-free. If $d \equiv 2, 3 \pmod{4}$, then $\mathbb{Z}[\sqrt{d}] = \mathcal{O}_d$ is a Dedekind domain and 2 ramifies in $\mathbb{Q}(\sqrt{d})$, so that $2\mathcal{O}_d = \mathfrak{p}^2$, where \mathfrak{p} is the unique prime ideal of \mathcal{O}_d dividing (2). Now suppose that $d \equiv 1 \pmod{4}$. Then $\mathcal{O}_d/\mathbb{Z}[\sqrt{d}]$ is an integral extension of rings, so by [Mat,

Theorem 9.3] any prime ideal of $\mathbb{Z}[\sqrt{d}]$ has the form $\mathbb{Z}[\sqrt{d}] \cap \mathfrak{p}$, where \mathfrak{p} is a prime ideal of \mathcal{O}_d . If $d \equiv 5 \pmod{8}$, then 2 is inert in $\mathbb{Q}(\sqrt{d})$; see [NZ, Theorem 9.29(4)]. Thus $2\mathcal{O}_d$ is prime and is the unique prime ideal of \mathcal{O}_d containing 2; this implies our claim by the previous observation. If $d \equiv 1 \pmod{8}$, then $2\mathcal{O}_d = \mathfrak{p}_1\mathfrak{p}_2 = \mathfrak{p}_1 \cap \mathfrak{p}_2$ for distinct prime ideals \mathfrak{p}_1 and \mathfrak{p}_2 of \mathcal{O}_d . Hence $\mathbb{Z}[\sqrt{d}] \cap \mathfrak{p}_1$ and $\mathbb{Z}[\sqrt{d}] \cap \mathfrak{p}_2$ each contain $I = \mathbb{Z}[\sqrt{d}] \cap 2\mathcal{O}_d = \{a + b\sqrt{d} : a \equiv b \pmod{2}\}$. Since I has index 2 in the ring $\mathbb{Z}[\sqrt{d}]$ and thus is a maximal ideal, it is the unique prime ideal of $\mathbb{Z}[\sqrt{d}]$ containing 2. \square

5.1. The case $d \equiv 2, 3 \pmod{4}$. If $d \equiv 2, 3 \pmod{4}$, then since the reduction mod 2 of a_d is the identity matrix, the reduction of $\underline{\mathbf{O}}_d/\underline{N}_d$ at (2) is nilpotent and contains only one point. Hence the finite group $\underline{\mathbf{O}}_d/\underline{N}_d$ must be isomorphic to $\underline{\mu}_2$. The resulting short exact sequence is

$$1 \rightarrow \underline{N}_d \rightarrow \underline{\mathbf{O}}_d \xrightarrow{\det} \underline{\mu}_2 \rightarrow 1. \quad (5.2)$$

Since $\det(\text{diag}(1, -1)) = -1$ and thus $\underline{\mathbf{O}}_d(\mathbb{Z}) \xrightarrow{\det} \{\pm 1\}$ is onto, flat cohomology yields the following exact sequence of pointed sets:

$$1 \rightarrow H_{\text{fl}}^1(\mathbb{Z}, \underline{N}_d) \xrightarrow{\delta} H_{\text{fl}}^1(\mathbb{Z}, \underline{\mathbf{O}}_d) \xrightarrow{\text{disc}} H_{\text{fl}}^1(\mathbb{Z}, \underline{\mu}_2) \cong \{\pm 1\}.$$

Here disc , which assigns to any class $[q] \in H_{\text{fl}}^1(\mathbb{Z}, \underline{\mathbf{O}}_d)$ the sign of the discriminant of q , is surjective because $[(1, 0, d)], [(1, 0, -d)] \in H_{\text{fl}}^1(\mathbb{Z}, \underline{\mathbf{O}}_d)$: observe that $(1, 0, d)$ becomes isomorphic to $(1, 0, -d)$ over $\mathbb{Z}[i]$ by the isometry $A = \text{diag}(1, i)$.

Lemma 5.4. *Let ${}^P\underline{\mathbf{O}}_d$ be the twisted form of $\underline{\mathbf{O}}_d$ by an \underline{N}_d -torsor P . Then the following are equivalent:*

- (1) *The map $H_{\text{fl}}^1(\mathbb{Z}, \underline{N}_d) \xrightarrow{\delta} H_{\text{fl}}^1(\mathbb{Z}, \underline{\mathbf{O}}_d)$ is injective.*
- (2) *The map ${}^P\underline{\mathbf{O}}_d(\mathbb{Z}) \xrightarrow{\det} \underline{\mu}_2(\mathbb{Z})$ is surjective for any $[P] \in H_{\text{fl}}^1(\mathbb{Z}, \underline{N}_d)$.*
- (3) *The $\underline{\mu}_2(\mathbb{Z})$ -action on $H_{\text{fl}}^1(\mathbb{Z}, \underline{N}_d)$ is trivial.*

Proof. Consider the exact and commutative diagram (cf. [Gir, III, Lemma 3.3.4])

$$\begin{array}{ccccccc} \underline{\mathbf{O}}_d(\mathbb{Z}) & \xrightarrow{\det} & \underline{\mu}_2(\mathbb{Z}) & \longrightarrow & H_{\text{fl}}^1(\mathbb{Z}, \underline{N}_d) & \xrightarrow{\delta} & H_{\text{fl}}^1(\mathbb{Z}, \underline{\mathbf{O}}_d) \\ & & & & \cong \downarrow \theta_P & & \cong \downarrow r \\ {}^P\underline{\mathbf{O}}_d(\mathbb{Z}) & \xrightarrow{\det} & \underline{\mu}_2(\mathbb{Z}) & \longrightarrow & H_{\text{fl}}^1(\mathbb{Z}, {}^P\underline{N}_d) & \xrightarrow{\delta'} & H_{\text{fl}}^1(\mathbb{Z}, {}^P\underline{\mathbf{O}}_d), \end{array}$$

where the map δ' is obtained by applying flat cohomology to the sequence (5.2) while replacing $\underline{\mathbf{O}}_d$ by the twisted group scheme ${}^P\underline{\mathbf{O}}_d$, and θ_P is the induced twisting bijection.

(1) \Leftrightarrow (2): The map δ is injective if any class $[P]$ of \underline{N}_d -torsors is the unique pre-image of $\delta([P]) \in H_{\text{fl}}^1(\mathbb{Z}, \underline{\mathbf{O}}_d)$. By commutativity of the diagram, this is equivalent to the distinguished point in $H_{\text{fl}}^1(\mathbb{Z}, {}^P\underline{N}_d)$ being the unique pre-image of its image, for any choice of a twisted form ${}^P\underline{N}_d$ of \underline{N}_d ,

i.e. to the triviality of $\ker(\delta')$ for any \underline{N}_d -torsor P . By exactness of the rows, this is condition (2).
(1) \Leftrightarrow (3): By [Gir, Proposition III.3.3.3(iv)], δ' induces an injection of $H_{\mathfrak{H}}^1(\mathbb{Z}, \underline{N}_d)/\underline{\mu}_2(\mathbb{Z})$ into $H_{\mathfrak{H}}^1(\mathbb{Z}, \underline{\mathbf{O}}_d)$. Thus $\delta : H_{\mathfrak{H}}^1(\mathbb{Z}, \underline{N}_d) \rightarrow H_{\mathfrak{H}}^1(\mathbb{Z}, \underline{\mathbf{O}}_d)$ is injective if and only if $\underline{\mu}_2(\mathbb{Z})$ acts on $H_{\mathfrak{H}}^1(\mathbb{Z}, \underline{N}_d)$ trivially. \square

Lemma 5.5. *If $d \equiv 2, 3 \pmod{4}$ then*

$$H_{\mathfrak{H}}^1(\mathbb{Z}, \underline{\mathbf{O}}_d) = (H_{\mathfrak{H}}^1(\mathbb{Z}, \underline{N}_d)/\sim) \coprod (H_{\mathfrak{H}}^1(\mathbb{Z}, \underline{N}'_{-d})/\sim),$$

where $H_{\mathfrak{H}}^1(\mathbb{Z}, \underline{N}_d)$ and $H_{\mathfrak{H}}^1(\mathbb{Z}, \underline{N}'_{-d})$ properly classify integral forms that are isomorphic in the flat topology to $(1, 0, -d)$ and $(1, 0, d)$, respectively, and the relation \sim is given by $[(a, b, c)] \sim [(a, -b, c)]$. Each of these groups is entirely embedded if and only if it satisfies one (hence all) of the conditions of Lemma 5.4.

Proof. The sequence (5.2) splits by Remark 5.2, so that $\underline{\mathbf{O}}_d \cong \underline{N}_d \rtimes \underline{\mu}_2$. By [Gil, Lemma 2.6.3] this implies the decomposition

$$H_{\mathfrak{H}}^1(\mathbb{Z}, \underline{\mathbf{O}}_d) = H_{\mathfrak{H}}^1(\mathbb{Z}, \underline{N}_d)/\underline{\mu}_2(\mathbb{Z}) \coprod H_{\mathfrak{H}}^1(\mathbb{Z}, \underline{N}'_{-d})/\underline{\mu}_2(\mathbb{Z}), \quad (5.3)$$

where \underline{N}'_{-d} is the special orthogonal group of the unique twisted quadratic form q'_{-d} corresponding to the non-trivial $\underline{\mu}_2$ -torsor represented by $\{t^2 = -1\}$, and the quotients are taken modulo the equivalence relation given by the action of $\underline{\mu}_2(\mathbb{Z})$ on each group. The form q'_{-d} is represented by

$$\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix},$$

hence $q'_{-d} = (1, 0, d)$ and $\text{disc}(q'_{-d}) = -\Delta_k$. The non-trivial element of $\underline{\mu}_2(\mathbb{Z})$ acts via conjugation by $\text{diag}(1, -1)$, so it maps a form (a, b, c) to its *opposite* $(a, -b, c)$. The rest follows from Lemma 5.4. \square

Remark 5.6. Set $\underline{\mathbf{O}}'_{-d} \simeq \underline{N}'_{-d} \rtimes \underline{\mu}_2$. Observe that if we start the argument of the previous proof from $H_{\mathfrak{H}}^1(\mathbb{Z}, \underline{\mathbf{O}}'_{-d})$, we obtain exactly the same decomposition. In particular, $H_{\mathfrak{H}}^1(\mathbb{Z}, \underline{\mathbf{O}}_d) \simeq H_{\mathfrak{H}}^1(\mathbb{Z}, \underline{\mathbf{O}}'_{-d})$ when $d \equiv 2, 3 \pmod{4}$.

Example 5.7. The set $H_{\mathfrak{H}}^1(\mathbb{Z}, \underline{N}_{11})$ contains $2h_{11} = 2$ classes $\{[\pm(1, 0, -11)]\}$, with no opposite couples; see Lemma 5.12 below. However, $H_{\mathfrak{H}}^1(\mathbb{Z}, \underline{N}'_{-11})$ contains $h'_{-11} = 6$ classes by [Bue, Ch.2, p.20]. Precisely, we have $H_{\mathfrak{H}}^1(\mathbb{Z}, \underline{N}'_{-11}) = \{[\pm(1, 0, 11)], [\pm(3, \pm 2, 4)]\}$. The pairs $(3, \pm 2, 4)$ and $(-3, \pm 2, -4)$ coincide in $H_{\mathfrak{H}}^1(\mathbb{Z}, \underline{\mathbf{O}}_d)$. Thus $|H_{\mathfrak{H}}^1(\mathbb{Z}, \underline{\mathbf{O}}_d)| = 2 + 4 = 6$.

Now suppose $d \equiv 3 \pmod{4}$, and $d \neq -1$. By Lemma 4.1, the special orthogonal group \underline{N}'_{-d} appearing in Lemma 5.5 is equal to $\underline{\mathbf{O}}_{\Omega}^+$ for $\Omega = \{1, \sqrt{-d}\}$. Set $k' = \mathbb{Q}(\sqrt{-d})$. Since $-d \equiv 1 \pmod{4}$, the order $\mathcal{O}_{\Omega} = \mathbb{Z}[\sqrt{-d}]$ is a proper subring of $\mathcal{O}_{k'} = \mathbb{Z}[\frac{1+\sqrt{-d}}{2}]$. We relate the Picard groups of

these rings by studying their localizations. For any prime ideal \mathfrak{p} of \mathcal{O}_Ω , let $\mathcal{O}_\mathfrak{p}$ be the localization of \mathcal{O}_Ω at \mathfrak{p} , and let $(\mathcal{O}_{k'})_\mathfrak{p}$ be the integral closure of $\mathcal{O}_\mathfrak{p}$ in $\mathcal{O}_{k'}$. Then [KP, Theorem 5.6] provides an exact sequence of abelian groups

$$1 \rightarrow \mathcal{O}_\Omega^\times \xrightarrow{\varphi} \mathcal{O}_{k'}^\times \rightarrow \bigoplus_{\mathfrak{p}} (\mathcal{O}_{k'})_\mathfrak{p}^\times / \mathcal{O}_\mathfrak{p}^\times \rightarrow \text{Pic}(\mathcal{O}_\Omega) \rightarrow \text{Pic}(\mathcal{O}_{k'}) \rightarrow 1. \quad (5.4)$$

Here the direct sum runs over the prime ideals of \mathcal{O}_Ω . Let \mathcal{F} denote the conductor of $\mathcal{O}_{k'}/\mathcal{O}_\Omega$, namely the largest ideal of \mathcal{O}_Ω which is also an ideal of $\mathcal{O}_{k'}$. By [KP, Proposition 6.2] we have the following isomorphism for any \mathfrak{p} :

$$(\mathcal{O}_{k'})_\mathfrak{p}^\times / \mathcal{O}_\mathfrak{p}^\times \cong ((\mathcal{O}_{k'})_\mathfrak{p} / \mathcal{F} \cdot (\mathcal{O}_{k'})_\mathfrak{p})^\times / (\mathcal{O}_\mathfrak{p} / \mathcal{F} \mathcal{O}_\mathfrak{p})^\times. \quad (5.5)$$

Since $\mathcal{O}_\Omega = \mathbb{Z} + 2\mathcal{O}_{k'}$, the conductor is $\mathcal{F} = 2\mathcal{O}_{k'}$. It is a maximal ideal of \mathcal{O}_Ω ; since localization at any prime commutes with factorization modulo \mathcal{F} , we have $(\mathcal{O}_\mathfrak{p} / \mathcal{F} \mathcal{O}_\mathfrak{p})^\times = (\mathcal{O}_\Omega / \mathcal{F} \mathcal{O}_\Omega)_\mathfrak{p}^\times = \mathbb{F}_2^\times = 1$. Moreover, we see that $(\mathcal{O}_{k'})_\mathfrak{p}^\times \cong \mathcal{O}_\mathfrak{p}^\times$ if $2 \notin \mathfrak{p}$, so such places make no contribution to the direct sum in (5.4). It remains therefore to compute $(\overline{\mathcal{O}_{k'}})_\mathfrak{q}^\times$ for the unique (see Lemma 5.3) place $2 \in \mathfrak{q}$, where $\overline{\mathcal{O}_{k'}}$ denotes the reduction of $\mathcal{O}_{k'}$ modulo \mathcal{F} . Note that $\mathcal{O}_\Omega / \mathfrak{q} \simeq \mathbb{F}_2$ and that $c = \frac{1+d}{4}$ is odd if $d \equiv 3 \pmod{8}$ and even if $d \equiv 7 \pmod{8}$. If $\bar{c} \in \mathbb{F}_2$ is the image of c , then it follows from (4.2) that

$$\begin{aligned} (\overline{\mathcal{O}_{k'}})_\mathfrak{q}^\times &\cong (\overline{R}_{-d}(\mathbb{F}_2))_\mathfrak{q} = \left\{ (\overline{A}_{-d})_\mathfrak{q} = \begin{pmatrix} a & \bar{c}b \\ b & a+b \end{pmatrix} : a, b \in \mathbb{F}_2, \det(\overline{A}_{-d}) \neq 0 \right\} \\ &\cong \begin{cases} \mathbb{Z}/3 & d \equiv 3 \pmod{8} \\ 1 & d \equiv 7 \pmod{8}. \end{cases} \end{aligned}$$

This holds also when $d = -1$. We deduce from (5.4) that if $d \equiv 7 \pmod{8}$, then $\text{Pic} \mathcal{O}_\Omega \simeq \text{Pic} \mathcal{O}_{-d}$. If $d \equiv 3 \pmod{8}$, then (5.4) implies that

$$\frac{|\text{Pic}(\mathcal{O}_\Omega)|}{h_{-d}} = \frac{3}{|\text{coker}(\varphi)|}. \quad (5.6)$$

If $d \neq 3$, the unit groups $\mathcal{O}_\Omega^\times$ and $\mathcal{O}_{k'}^\times$ contain the same roots of unity. Moreover, if $d > 0$, these groups have no free part, hence $|\text{coker}(\varphi)| = 1$. If $d = 3$, then clearly $|\text{coker}(\varphi)| = 3$. If $d < 0$, then the free parts of both $\mathcal{O}_\Omega^\times$ and $\mathcal{O}_{k'}^\times$ have rank 1, and $\text{coker}(\varphi) = [\langle \varepsilon \rangle : \langle \varepsilon^m \rangle] = m$, where ε is a fundamental unit of k' and ε^m is a generator of $\mathcal{O}_\Omega^\times$. Note that $m|3$ by (5.4), so that $m = 3$ or $m = 1$. The case $m = 1$ occurs, for instance, when $d = -37$ and $d = -101$; see sequence A108160 in the *On-Line Encyclopedia of Integer Sequences*.

Corollary 5.8. *Let $d \equiv 3 \pmod{4}$. Set $\eta(d) = 1$ if $d \equiv 3 \pmod{8}$ and one of the following two conditions holds:*

- $d > 3$
- $d < 0$ and $\mathcal{O}_{-d}^\times \subset \mathbb{Z}[\sqrt{-d}]$.

Otherwise, set $\eta(d) = 0$. Then $|\text{Pic } \mathbb{Z}[\sqrt{-d}]| = 3^{\eta(d)} \cdot h_{-d}$.

If the norm map $N_{k/\mathbb{Q}}$ attains the value -1 for any element of $\mathcal{O}_\Omega^\times$, it does so for a generator of its free part. As m is odd, this implies that $N_{k/\mathbb{Q}}(\mathcal{O}_{k'}^\times) = N_{k/\mathbb{Q}}(\mathcal{O}_\Omega^\times)$. Thus (2.3) and Corollary 5.8 show that

$$\frac{|H_{\mathfrak{f}}^1(\mathbb{Z}, \underline{N}'_{-d})|}{|H_{\mathfrak{f}}^1(\mathbb{Z}, \underline{N}_{-d})|} = \frac{|\text{Pic } \mathbb{Z}[\sqrt{-d}]|}{h_{-d}} = 3^{\eta(d)}. \quad (5.7)$$

Example 5.9. We tabulate the following data from [Bue]: see page 19 for the second and fourth columns and page 20 for the third, noting that, as the forms obtained are definite, the number of total classes is double the number of positive classes by Proposition 5.13 below.

$0 < d \equiv 3(\text{mod } 4)$	h_{-d}	$ H_{\mathfrak{f}}^1(\mathbb{Z}, \underline{N}'_{-d}) $	$ H_{\mathfrak{f}}^1(\mathbb{Z}, \underline{N}_{-d}) $	$c = \frac{1+d}{4}$
3	1	2	2	1
7	1	2	2	2
11	1	6	2	3
15	2	4	4	4
19	1	6	2	5
23	3	6	6	6

Example 5.10. Let $d = -5$. Then $(\overline{\mathcal{O}}_{k'})_{(2)}^\times / \overline{\mathcal{O}}_{(2)}^\times \cong \mathbb{Z}/3$ by the argument preceding (5.6). Since $\frac{1+\sqrt{5}}{2} \in \mathcal{O}_{-d}$ is a unit, we have $\eta(d) = 0$. Indeed, the embedding $\varphi : \mathcal{O}_\Omega \rightarrow \mathcal{O}_{k'}$ is given, in the integral matrix realization of (4.2), by the linear transformation

$$\varphi : \begin{pmatrix} x & 5y \\ y & x \end{pmatrix} \mapsto \begin{pmatrix} x-y & 2y \\ 2y & x+y \end{pmatrix}.$$

Writing $\text{free}(\underline{N}'_5(\mathbb{Z})) = (z)$ and $\text{free}(\underline{N}_5(\mathbb{Z})) = (u)$, where

$$z = \begin{pmatrix} 2 & 5 \\ 1 & 2 \end{pmatrix} \text{ and } u = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \text{ we get } \varphi(z) = \begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix} = u^3.$$

We have $|H_{\mathfrak{f}}^1(\mathbb{Z}, \underline{N}'_{-5})| = |H_{\mathfrak{f}}^1(\mathbb{Z}, \underline{N}_{-5})| = 2h_{-5}^+ = 2h_{-5} = 4$, where the first equality is (5.7) and the second is (2.8). Indeed, $H_{\mathfrak{f}}^1(\mathbb{Z}, \underline{N}'_{-5}) = \{\pm[(1, 0, 5)], \pm[(2, 2, 3)]\}$ by [Bue, p.20].

5.2. The case $d \equiv 1(\text{mod } 4)$. When $d \equiv 1(\text{mod } 4)$, a different behavior is exhibited. In this case, $\underline{\mathbf{O}}_d/\underline{N}_d$ contains two points also at the reduction at (2), as the reduction of a_d modulo 2 is not the identity by (5.1). Thus $\underline{\mathbf{O}}_d/\underline{N}_d$ must be isomorphic to $(\mathbb{Z}/2)_{\mathbb{Z}}$. Moreover, the norm form q_d defined in (4.1) is unimodular in this case, i.e. non-degenerate locally everywhere. Hence the natural projection $D_{q_d} : \underline{\mathbf{O}}_d \rightarrow (\mathbb{Z}/2)_{\mathbb{Z}}$ is the Dickson epimorphism (see [BCon, Prop. 1.5] for its definition). Applying flat cohomology to the resulting short exact sequence

$$1 \rightarrow \underline{N}_d \rightarrow \underline{\mathbf{O}}_d \xrightarrow{D_{q_d}} (\mathbb{Z}/2)_{\mathbb{Z}} \rightarrow 1$$

yields the exact sequence of pointed sets

$$1 \rightarrow H_{\mathfrak{H}}^1(\mathbb{Z}, \underline{N}_d) \xrightarrow{i} H_{\mathfrak{H}}^1(\mathbb{Z}, \underline{\mathbf{O}}_d) \xrightarrow{\delta} H_{\mathfrak{H}}^1(\mathbb{Z}, (\mathbb{Z}/2)_{\mathbb{Z}}). \quad (5.8)$$

The left exactness is due to the surjectivity of $D_{q_d} : \underline{\mathbf{O}}_d(\mathbb{Z}) \rightarrow \mathbb{Z}/2 = \{0, 1\}$, as a_d has non-trivial reduction modulo 2. Since $(\mathbb{Z}/2)_{\mathbb{Z}}$ is smooth, the rightmost term coincides with $H_{\text{ét}}^1(\mathbb{Z}, (\mathbb{Z}/2)_{\mathbb{Z}})$ by [SGA4, Corollaire VIII.2.3], and the induced map δ assigns to any class $[q] \in H_{\mathfrak{H}}^1(\mathbb{Z}, \underline{\mathbf{O}}_d)$ an étale double cover of \mathbb{Z} (cf. [BCon, p.6]), whence δ is trivial as \mathbb{Z} admits no such cover. This also means that the classification in $H_{\mathfrak{H}}^1(\mathbb{Z}, \underline{\mathbf{O}}_d)$ is only proper, so together with $\ker(i) = 1$, this implies that i is injective. We have established the following.

Corollary 5.11. *If $d \equiv 1 \pmod{4}$, there is an isomorphism of abelian groups $H_{\mathfrak{H}}^1(\mathbb{Z}, \underline{N}_d) \cong H_{\mathfrak{H}}^1(\mathbb{Z}, \underline{\mathbf{O}}_d)$.*

As mentioned in the introduction, Gauss showed that the proper isomorphism classes of forms of discriminant Δ_k are parametrized by $\text{Pic}^+(\mathcal{O}_k)$. If $d < 0$, this classification treats only positive definite forms, i.e. those for which $a, c > 0$. The following lemma completes the proper classification.

Lemma 5.12. *If $d \notin \{0, 1\}$ is a square-free integer, then $H_{\mathfrak{H}}^1(\mathbb{Z}, \underline{N}_d) = \{\pm 1\}^{\mu(d)} \times \text{Pic}^+(\mathcal{O}_k)$, where*

$$\mu(d) = \begin{cases} 1 & d < 0 \\ 0 & d > 0. \end{cases}$$

Proof. By Lemma 4.1 we have $H_{\mathfrak{H}}^1(\mathbb{Z}, \underline{N}_d) = H_{\mathfrak{H}}^1(\mathbb{Z}, \underline{\mathbf{O}}_d^+)$, and the latter properly classifies the integral quadratic forms that are locally isomorphic to q_d for the flat topology, thus of discriminant Δ_k . So if $d > 0$, then $H_{\mathfrak{H}}^1(\mathbb{Z}, \underline{N}_d)$ naturally injects into $\text{Pic}^+(\mathcal{O}_k)$, which properly classifies all binary quadratic forms of discriminant Δ_k by classical work of Gauss [FT, Theorem 58]. Since $H_{\mathfrak{H}}^1(\mathbb{Z}, \underline{N}_d)$ and $\text{Pic}^+(\mathcal{O}_k)$ have the same cardinality by (2.8), we have obtained a natural bijection between them.

If $d < 0$, however, then $\text{Pic}^+(\mathcal{O}_k)$ classifies only the **positive** definite forms (see the proof referenced above of the theorem of Gauss). So the subset $H_{\mathfrak{H}}^1(\mathbb{Z}, \underline{N}_d)^+$ of classes of positive forms injects into $\text{Pic}^+(\mathcal{O}_k) = \text{Pic } \mathcal{O}_k$. If $[q] \in H_{\mathfrak{H}}^1(\mathbb{Z}, \underline{N}_d)$, then the isometry $\text{diag}(\sqrt{-1}, \sqrt{-1})$ shows that $[-q]$ belongs to $H_{\mathfrak{H}}^1(\mathbb{Z}, \underline{\mathbf{O}}_d)$. Thus $[-q] \in H_{\mathfrak{H}}^1(\mathbb{Z}, \underline{N}_d)$ by Corollary 5.11. Furthermore, since q realizes only non-negative values and $-q$ realizes non-positive values, the two forms q and $-q$ cannot be \mathbb{Z} -equivalent. Since every definite form is positive or negative, we have $\{\pm 1\} \times H_{\mathfrak{H}}^1(\mathbb{Z}, \underline{N}_d)^+ = H_{\mathfrak{H}}^1(\mathbb{Z}, \underline{N}_d)$, and we have just shown that this injects into $\{\pm 1\} \times \text{Pic}^+(\mathcal{O}_k)$. Again by (2.8), these sets have the same cardinality, so our injection is a bijection. \square

Proposition 5.13. *For any square-free integer $d \notin \{0, 1\}$, the abelian group $\text{Pic}^+(\mathbb{Z}[\sqrt{d}])$ properly classifies the integral forms isomorphic to $(1, 0, d)$ in the flat topology (only positive definite if $d < 0$) via: $[(a, b, c)] \mapsto [(a, b\sqrt{d})]$, and $\{\pm 1\}^{\mu(d)} \times \text{Pic}^+(\mathbb{Z}[\sqrt{d}])$ classifies also the negative definite forms.*

Proof. If $d \equiv 2, 3 \pmod{4}$, then $\mathbb{Z}[\sqrt{d}] = \mathcal{O}_k$ and the claim is Lemma 5.12. So assume $d \equiv 1 \pmod{4}$ and set $\Omega = \{1, \sqrt{d}\}$. We first show that $H_{\mathfrak{h}}^1(\mathbb{Z}, \mathbf{O}_{\Omega}^+)^+ \cong \text{Pic}^+(\mathbb{Z}[\sqrt{d}])$. The morphism of \mathbb{Z} -groups $\varphi : \underline{R}_{\Omega} = \text{Spec } \mathbb{Z}[x, y, t^{-1}]/(x^2 - dy^2 - t) \rightarrow \underline{R}_d = \text{Spec } \mathbb{Z}[a, b, t^{-1}]/(a^2 + ab + cb^2 - t)$ defined by $(a, b, t) \mapsto (x - y, 2y, t)$, via their integral matrix representations (similarly to (4.2)) is

$$\varphi : \begin{pmatrix} x & dy \\ y & x \end{pmatrix} \mapsto \begin{pmatrix} x - y & -2cy \\ 2y & x + y \end{pmatrix}. \quad (5.9)$$

It induces an embedding of the groups of units $\varphi_{\mathbb{Z}} : \underline{R}_{\Omega}(\mathbb{Z}) \cong \mathcal{O}_{\Omega}^{\times} \hookrightarrow \underline{R}_d(\mathbb{Z}) \cong \mathcal{O}_k^{\times}$, thus also a surjection $i_* : \text{Pic } \mathbb{Z}[\sqrt{d}] \rightarrow \text{Pic } \mathcal{O}_k$ (cf. (5.4)). Since φ preserves the determinant it can be restricted to $\varphi : \underline{N}_{\Omega} \rightarrow \underline{N}_d$. This only fails to be an isomorphism of group schemes locally at (2), where it is not even a monomorphism. Restricting to the small site of flat extensions, the sheafifications $\tilde{\underline{N}}_{\Omega}$ and $\tilde{\underline{N}}_d$ admit, due to the flatness of their associated schemes, the following diagram of abelian groups for any flat extension R of \mathbb{Z} :

$$\begin{array}{ccc} \tilde{\underline{N}}_{\Omega}(R) & \xrightarrow{\tilde{\varphi}_R} & \tilde{\underline{N}}_d(R) \\ \parallel & & \parallel \\ \underline{N}_{\Omega}(R) & \xrightarrow{\varphi_R} & \underline{N}_d(R) \\ \downarrow & & \downarrow \\ N(\mathbb{Q}) & \xrightarrow{\cong} & N(\mathbb{Q}). \end{array}$$

We deduce that $\tilde{\varphi} : \tilde{\underline{N}}_{\Omega} \rightarrow \tilde{\underline{N}}_d$ is a monomorphism of sheaves and that the quotient $Q = \tilde{\underline{N}}_d / \tilde{\underline{N}}_{\Omega}$ has a support in the (2)-fiber only. Flat cohomology then yields the exactness of

$$1 \rightarrow \tilde{\underline{N}}_{\Omega}(\mathbb{Z}) \xrightarrow{\tilde{\varphi}_{\mathbb{Z}}} \tilde{\underline{N}}_d(\mathbb{Z}) \rightarrow Q(\mathbb{Z}) \rightarrow H_{\mathfrak{h}}^1(\mathbb{Z}, \underline{N}_{\Omega}) \xrightarrow{\varphi_*} H_{\mathfrak{h}}^1(\mathbb{Z}, \underline{N}_d) \rightarrow H_{\mathfrak{h}}^1(\mathbb{Z}, Q). \quad (5.10)$$

We saw after Corollary 5.8 that $N_{k/\mathbb{Q}}(\mathcal{O}_{\Omega}^{\times}) = N_{k/\mathbb{Q}}(\mathcal{O}_k^{\times})$, so the two exact sequences of abelian groups associated to Ω and $\{1, \omega\}$ in (2.3) are related by the exact and commutative diagram

$$\begin{array}{ccccccc} 1 & \longrightarrow & \{\pm 1\}/N_{k/\mathbb{Q}}(\mathcal{O}_{\Omega}^{\times}) & \longrightarrow & H_{\mathfrak{h}}^1(\mathbb{Z}, \underline{N}_{\Omega}) & \xrightarrow{(i_{\Omega})_*} & \text{Pic } (\mathbb{Z}[\sqrt{d}]) \longrightarrow 1 \\ & & \parallel & & \downarrow \varphi_* & & \downarrow i_* \\ 1 & \longrightarrow & \{\pm 1\}/N_{k/\mathbb{Q}}(\mathcal{O}_k^{\times}) & \longrightarrow & H_{\mathfrak{h}}^1(\mathbb{Z}, \underline{N}_d) & \xrightarrow{(i_d)_*} & \text{Pic } (\mathcal{O}_k) \longrightarrow 1 \end{array} \quad (5.11)$$

Since i_* is surjective, a diagram chase shows that φ_* is surjective as well. Lemma 5.12 identifies $\{\pm 1\}^{\mu(d)} \times \text{Pic}^+(\mathcal{O}_k)$ with $H_{\mathfrak{h}}^1(\mathbb{Z}, \underline{N}_d)$. By Lemma 4.1, the pointed set $H_{\mathfrak{h}}^1(\mathbb{Z}, \underline{N}_{\Omega})$ is equal to the

proper classification $H_{\mathfrak{H}}^1(\mathbb{Z}, \mathbf{O}_{\Omega}^+)$. We claim that $\text{Pic}^+(\mathbb{Z}[\sqrt{d}])$ embeds naturally in $H_{\mathfrak{H}}^1(\mathbb{Z}, \underline{N}_{\Omega})$ and that $\varphi_*^{-1}(\text{Pic}^+(\mathcal{O}_k)) = \text{Pic}^+(\mathbb{Z}[\sqrt{d}])$. This will imply that φ_* is an extension of i_* .

If $d < -3$, then $\mathcal{O}_{\Omega}^{\times} = \mathcal{O}_k^{\times}$ and φ_* is a bijection, so that $Q(\mathbb{Z}) = 1$. In fact, φ_* maps the class of the base point $(1, 0, -d)$ to the class of $(1, 1, c)$; more generally, since $\underline{\mathbf{O}}_{\Omega}^+ = \underline{N}_{\Omega}$, any form twisted by a (not necessarily self) isometry $g \in \underline{\mathbf{SL}}_2(\overline{\mathbb{Z}})$ is mapped to the corresponding twisting:

$$\varphi_* : \left[g^t \begin{pmatrix} 1 & 0 \\ 0 & -d \end{pmatrix} g \right] \mapsto \left[g^t \begin{pmatrix} 1 & 1/2 \\ 1/2 & c \end{pmatrix} g \right].$$

Explicitly, for $g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ this reads

$$\varphi_* : \left[\left(N_{k/\mathbb{Q}}(\alpha + \gamma\sqrt{d}), *, N_{k/\mathbb{Q}}(\beta + \delta\sqrt{d}) \right) \right] \mapsto \left[\left(N_{k/\mathbb{Q}}(\alpha + \gamma\omega), *, N_{k/\mathbb{Q}}(\beta + \delta\omega) \right) \right].$$

Set $A = \begin{pmatrix} \alpha & d\gamma \\ \gamma & \alpha \end{pmatrix} \in \underline{R}_{\Omega}(\overline{\mathbb{Z}})$ and observe that $N_{k/\mathbb{Q}}(\alpha + \gamma\sqrt{d}) = \det A$, while $N_{k/\mathbb{Q}}(\alpha + \gamma\omega) = \det(\varphi(A) \in \underline{R}_d(\overline{\mathbb{Z}}))$. Since φ preserves determinants by (5.9), this implies that only positive definite forms in $H_{\mathfrak{H}}^1(\mathbb{Z}, \underline{N}_{\Omega})$ are mapped by φ_* to positive definite forms in $H_{\mathfrak{H}}^1(\mathbb{Z}, \underline{N}_d)$. Hence $\varphi_*^{-1}(\text{Pic}(\mathcal{O}_k)) = \text{Pic}(\mathbb{Z}[\sqrt{d}])$, as claimed.

If $d > 0$, then $H_{\mathfrak{H}}^1(\mathbb{Z}, \underline{N}_d)$ is identified with $\text{Pic}^+(\mathcal{O}_k)$. If $N_{k/\mathbb{Q}}(\mathcal{O}_{\Omega}^{\times}) = \{\pm 1\}$, then $\text{Pic}^+(\mathcal{O}_k) = \text{Pic} \mathcal{O}_k$ and the claim is obvious. Otherwise, $N_{k/\mathbb{Q}}(\mathcal{O}_{\Omega}^{\times}) = \{1\}$ and the diagram (5.11) becomes

$$\begin{array}{ccccccc} 1 & \longrightarrow & \{\pm 1\} & \longrightarrow & H_{\mathfrak{H}}^1(\mathbb{Z}, \underline{N}_{\Omega}) & \xrightarrow{(i_{\Omega})_*} & \text{Pic}(\mathbb{Z}[\sqrt{d}]) \longrightarrow 1 \\ & & \parallel & & \downarrow \varphi_* & & \downarrow i_* \\ 1 & \longrightarrow & \{\pm 1\} & \longrightarrow & \text{Pic}^+(\mathcal{O}_k) & \xrightarrow{(i_d)_*} & \text{Pic}(\mathcal{O}_k) \longrightarrow 1, \end{array}$$

where $(i_d)_*$ multiplies ideals by the subgroup of all principal ideals in \mathcal{O}_k (not only the totally positive ones), and $\varphi_* : \mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_k$ extends ideals by extending the integral basis from $\{1, \sqrt{d}\}$ to $\{1, \frac{1+\sqrt{d}}{2}\}$ (see before [KP, Theorem 5.6] and recall that $d \equiv 1 \pmod{4}$). By the commutativity of the diagram, these two operations commute. Thus $\varphi_*^{-1}(\text{Pic}^+(\mathcal{O}_k)) \simeq \text{Pic}^+(\mathbb{Z}[\sqrt{d}])$, as claimed.

Gauss identified $H_{\mathfrak{H}}^1(\mathbb{Z}, \underline{N}_d)^+$ with $\text{Pic}^+(\mathcal{O}_k)$ via the map $[(a, b, c)] \mapsto [(a, \frac{b+\sqrt{d}}{2})]$. We have shown that the composition of φ_* with Gauss' map is an extension of i_* to $\text{Pic}^+(\mathbb{Z}[\sqrt{d}])$. Noting that $i_*([\sqrt{d}]) = [\omega]$, the asserted map fits into the commutative diagram

$$\begin{array}{ccc} H_{\mathfrak{H}}^1(\mathbb{Z}, \underline{N}_{\Omega})^+ & \xrightarrow[\sim]{[(a,b,c)] \mapsto [(a,b\sqrt{d})]} & \text{Pic}^+(\mathbb{Z}[\sqrt{d}]) \\ \downarrow \varphi_* & & \downarrow \sqrt{d} \mapsto \omega \\ H_{\mathfrak{H}}^1(\mathbb{Z}, \underline{N}_d)^+ & \xrightarrow[\sim]{[(a,b,c)] \mapsto [(a, \frac{b+\sqrt{d}}{2})]} & \text{Pic}^+(\mathcal{O}_k) \end{array}$$

and it is an isomorphism of abelian groups, being a lift of the Gauss' one. \square

5.3. Conclusions. Having studied the cases $d \equiv 1 \pmod{4}$ and $d \equiv 2, 3 \pmod{4}$ separately, we gather together our results. Let $d \notin \{0, 1\}$ be a square-free integer.

Proposition 5.14. *Let m_d be the number of opposite pairs $[(a, \pm b, c)]$ contained in $\text{Pic}^+(\mathcal{O}_k)$, and let l_d be the number of such pairs in $\text{Pic } \mathbb{Z}[\sqrt{-d}]$. Let h_d^+ be the narrow class number of $\mathbb{Q}(\sqrt{d})$. Then*

$$|H_{\mathbb{R}}^1(\mathbb{Z}, \underline{\mathbf{O}}_d)| = \begin{cases} 2^{\mu(d)} h_d^+ & d \equiv 1 \pmod{4} \\ 2^{\mu(d)} h_d^+ + 2^{\mu(-d)} h_{-d}^+ - m_d - l_d & d \equiv 2 \pmod{4} \\ 2^{\mu(d)} h_d^+ + 2^{\mu(-d)} \cdot 3^{\eta(d)} h_{-d}^+ - m_d - l_d & d \equiv 3 \pmod{4}. \end{cases}$$

Proof. If $d \equiv 1 \pmod{4}$ then $|H_{\mathbb{R}}^1(\mathbb{Z}, \underline{\mathbf{O}}_d)| = |H_{\mathbb{R}}^1(\mathbb{Z}, \underline{N}_d)| = h_d^+ \cdot 2^{\mu(d)}$, where the first equality is Corollary 5.11 and the second comes from (2.8). Otherwise, use Lemma 5.5 and notice that if $d \equiv 2 \pmod{4}$, then $-d \equiv 2 \pmod{4}$ as well, so $\underline{N}'_{-d} = \underline{N}_{-d}$. On the other hand, if $d \equiv 3 \pmod{4}$, then $-d \equiv 1 \pmod{4}$, and the claim follows from (5.7). \square

The following corollary may be viewed as an extension of the theorem of Gauss stating that the composition of any class in $\text{Pic}^+(\mathcal{O}_k)$, of any genus, with itself belongs to the principal genus. See [Knu, p. 310] for details.

Corollary 5.15. *For any class $[q] \in H_{\mathbb{R}}^1(\mathbb{Z}, \underline{\mathbf{O}}_d^+)$, the class $[q \otimes q]$ belongs to the principal genus.*

Proof. We have seen in (3.4) that $H_{\mathbb{R}}^1(\mathbb{Z}_p, (\underline{N}_d)_p)$ injects into $H^1(\mathbb{Q}_p, N_p)$ for any p . As a result, by Remark 3.1 and (4.1) we obtain that

$$\text{Cl}_{\infty}(\underline{\mathbf{O}}_d^+) = \text{Cl}_{\infty}(\underline{N}_d) = \ker[H_{\mathbb{R}}^1(\mathbb{Z}, \underline{N}_d = \underline{\mathbf{O}}_d^+) \rightarrow H^1(\mathbb{Q}, N)],$$

showing that $\text{Cl}_{\infty}(\underline{\mathbf{O}}_d^+)$ is the principal genus of q . Moreover, the quotient $H_{\mathbb{R}}^1(\mathbb{Z}, \underline{N}_d)/\text{Cl}_{\infty}(\underline{N}_d) = \text{III}_{S_r \cup \{\infty\}}^1(\mathbb{Q}, N)$ has exponent 2 by Corollary 3.2 and Remark 3.3. Recall that \underline{N}_d is commutative. Thus for any class $[q]$ in the group $H_{\mathbb{R}}^1(\mathbb{Z}, \underline{N}_d)$, the class of the tensor product $q \otimes q$ lies in $\text{Cl}_{\infty}(\underline{N}_d) = \text{Cl}_{\infty}(\underline{\mathbf{O}}_d^+)$. \square

Remark 5.16. Corollary 3.2 shows that $\text{Cl}_{\infty}(\underline{N}_d)$ embeds as a subgroup in $H_{\mathbb{R}}^1(\mathbb{Z}, \underline{N}_d)$. The latter group is a disjoint union of classes of integral quadratic binary forms of discriminant Δ_k of all genera. This embedding holds for any twisted form of q_d , hence the quotient $H_{\mathbb{R}}^1(\mathbb{Z}, \underline{N}_d)/\text{Cl}_{\infty}(\underline{N}_d) \simeq \text{III}_{S_r \cup \{\infty\}}^1(\mathbb{Q}, N_d)$ is in bijection with the set of proper genera of q_d . Hence there are $2^{|S_r|-1}$ such proper genera, as was initially proved by Gauss; see also [Ono2, §5, Example 2] and [Wat, Corollary 16].

REFERENCES

- [SGA4] M. Artin, A. Grothendieck, J.-L. Verdier, *Théorie des Topos et Cohomologie Étale des Schémas* (SGA 4) LNM, Springer, 1972/1973.
- [BP] A. Borel, G. Prasad, *Finiteness theorems for discrete subgroups of bounded covolume in semi-simple groups*, Publ. Math. IHES **69** (1989), 119–171.
- [BLR] S. Bosch, W. Lütkebohmert, M. Raynaud, *Néron Models*, Springer, Berlin, 1990.
- [Bou] N. Bourbaki, *Éléments of Mathematics, Commutative Algebra*, Hermann, Paris, 1972.
- [Bue] D. A. Buell, *Binary Quadratic Forms, Classical Theory and Modern Computations*, Springer-Verlag, 1989.
- [BCon] B. Conrad, *Math 252. Properties of orthogonal groups*, [http://math.stanford.edu/~conrad/252Page/handouts/O\(q\).pdf](http://math.stanford.edu/~conrad/252Page/handouts/O(q).pdf)
- [KCon] K. Conrad, *History of class field theory*, <http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/cfthistory.pdf>
- [SGA3] M. Demazure, A. Grothendieck, *Séminaire de Géométrie Algébrique du Bois Marie - 1962-64 - Schémas en groupes*, Tome I, Réédition de SGA3 (2011), P. Gille, P. Polo.
- [FT] A. Frohlich, M. J. Taylor *Algebraic Number Theory*, Cambridge Studies in Advanced Mathematics 27.
- [Gau] C. F. Gauss, *Disquisitiones Arithmeticae*, 1801.
- [GP] P. Gille, A. Pianzola, *Isotriviality and étale cohomology of Laurent polynomial rings*, Journal of Pure and Applied Algebra **212** (2008), 780–800.
- [Gil] P. Gille, *Sur la classification des schémas en groupes semi-simples*. In “Autour des schémas en groupes” vol. III. Panorames et synthèses 47, 39-110. Paris, Société Mathématique de France, 2015.
- [Gir] J. Giraud, *Cohomologie non abélienne*, Grundlehren math. Wiss., Springer-Verlag Berlin Heidelberg New York, 1971.
- [KP] J. Kluners, S. Pauli, *Computing residue class rings and Picard groups of orders*, J. Algebra **292** (2005), 47–64.
- [Knu] M. A. Knus, *Quadratic and hermitian forms over rings*, Grundlehren der mat. Wissenschaften **294** (1991), Springer.
- [Lan] S. Lang, *Algebraic Number Theory*, Addison-Wesley, Reading, Mass., 1970.
- [Mat] H. Matsumura, *Commutative Ring Theory*, 2nd ed. Cambridge Studies in Advanced Mathematics 8. Cambridge Univ. Press, Cambridge, 1989.
- [Mil] J. Milne, *Class Field Theory*, May 6, 1997; v3.1.
- [Mor] M. Morishita, *On S -class number relations of algebraic tori in Galois extensions of global fields*, Nagoya Math. J. **124** (1991), 133–144.
- [Nis] Y. Nisnevich, *Étale Cohomology and Arithmetic of Semisimple Groups*, PhD thesis, Harvard University, 1982.
- [NZ] I. Niven, H. S. Zuckerman, *An introduction to the theory of Numbers*, 4th Ed. J. Wiley, New York, Chichester, Brisbane, Toronto 1980.
- [Ono1] T. Ono, *On the Tamagawa number of algebraic tori*, Annals of Mathematics **78** (1963), 47–63.
- [Ono2] T. Ono, *On some class number relations for Galois extensions*. Nagoya Math J. **107** (1987), 121–133.
- [PR] V. Platonov, A. Rapinchuk, *Algebraic Groups and Number Theory*, Academic Press, San Diego 1994.
- [TO] J. Tate, F. Oort, *Group schemes of prime order*, Ann. Sci. Ecole Norm. Sup. **3** (1970), 1–21.
- [Wat] W. C. Waterhouse, *Composition of norm-type forms*, J. Reine Angew. Math. **353** (1984), 85–97.

INSTITUT CAMILLE JORDAN, UNIVERSITÉ CLAUDE BERNARD LYON 1, 43 BOULEVARD DU 11 NOVEMBRE 1918,
F-69622 VILLEURBANNE CEDEX, FRANCE

E-mail address: rony.bitan@gmail.com

DEPARTMENT OF MATHEMATICS, BAR-ILAN UNIVERSITY, RAMAT GAN 5290002, ISRAEL

E-mail address: mschein@math.biu.ac.il